ブール多項式環における一変数最小多項式の計算について (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

井上, 秀太郎; 佐藤, 洋祐

数理解析研究所講究録
第1814巻 2012年 70-73

ブール多項式環における一変数最小多項式の計算について

井上　秀太郎
Shutaro Inoue
東京理科大学理学部
Department of Mathematical Information Science, Tokyo University of Science*

佐藤　洋祐
Yosuke Sato
東京理科大学理学部
Department of Mathematical Information Science, Tokyo University of Science†

1　はじめに

多項式環 $K[\bar{X}]$ 上のイデアルに対してある変数の最小多項式を求める場合、その変数を他の変数より順序を下げた消去順序でグレブナ基底を計算する必要がある. つまり、それぞれの変数に対する最小多項式を求める場合は複数回のグレブナ基底の計算を行うことになる. 本稿では、ブール多項式環上の一変数最小多項式が任意の単項式順序でのブーリアングレブナ基底から得られることを紹介する. この方法によってそれぞれの変数に対する最小多項式を同時に求めることができる.

2　ブール多項式環

ブール環とブール多項式環を次のように定義する.

定義 1 全ての要素が冪等であるような、単位元をもつ可換環 $\mathbf{B}$ をブール環とよぶ.

定義 2 ブール環 $\mathbf{B}$ を係数とする多項式環 $\mathbf{B}[X_1,\ldots,X_n]$ のイデアル $\langle X_1^2-X_1,\ldots,X_n^2-X_n\rangle$ による剰余環をブール多項式環とよび、$\mathbf{B}(X_1,\ldots,X_n)$ で表す.

ブール多項式に関しては拡張定理と零点定理が成り立つ.

定理 1 (拡張定理) I をブール多項式環 $\mathbf{B}(\bar{A},\bar{X})$ のイデアルとする. このとき任意の $\bar{a}\in V(I\cap\mathbf{B}(\bar{X}))$ にたいして $(\bar{a},\bar{b})\in V(I)$ となる $\bar{b}$ が存在する.

定理 2 (零点定理) I をブール多項式環 $\mathbf{B}(\bar{X})$ のイデアルとする. このとき

$$V(I)=\emptyset\Leftrightarrow\exists a\in\mathbf{B}\ a\in I\quad(\text{弱形の零点定理})$$

*sinoue@rs.kagu.tus.ac.jp
†ysato@rs.kagu.tus.ac.jp

が成り立つ. また I が有限生成であると仮定する. このとき

$$f(\bar{X}) \in I \Leftrightarrow \forall \bar{a} \in V(I)\ f(\bar{a}) = 0 \quad (\text{強形の零点定理})$$

が成り立つ.

3 ブーリアングレブナ基底

まず始めに係数ブール環上の多項式環でのグレブナ基底について説明する. 以降は次の記号を使用する. ある順序に対してブール多項式 f の最大の単項式を $LM(f)$ で表し,$LM(f)$ の係数と項をそれぞれ $LC(f)$ と $LT(f)$ で表す. また $f - LM(f)$ を $Rd(f)$ で表す.

定義 3 ブール多項式環 $\mathbf{B}[\bar{X}]$ のイデアル I に対して,I の有限部分集合 G が I のグレブナ基底であるとは $\langle LM(I)\rangle = \langle LM(G)\rangle$ を満たすことである.

定義 4 ブール多項式 $f = a\alpha + h \in \mathbf{B}[\bar{X}]$ による単項式簡約 $\rightarrow_f$ を

$$b\alpha\beta \rightarrow_f b(1+a)\alpha\beta + ba\beta h$$

と定義する.
(ただし $a = LC(f), b \in \mathbf{B}, ab \neq 0$ とし,$\alpha = LT(f), \beta \in T(\bar{X}), h = Rd(f)$ とする.)

係数ブール環上のグレブナ基底の計算には次の定義が必要になる.

定義 5 多項式 f が $lc(f)f = f$ を満たすとき f はブール閉であるという. $lc(f)f$ を f のブール閉包とよび、$bc(f)$ で表す.

一般の係数体のときと違い, 簡約グレブナ基底は一意性をもたない. よって新しい条件を加える.

定義 6 G を既約グレブナ基底とする. 任意の異なる多項式 $f, g \in G$ にたいして $LT(f) \neq LT(g)$ が成り立つとき G は *stratified* であるとよぶ.

定理 3 G, H を $\langle G\rangle = \langle H\rangle$ を満たす *stratified* なグレブナ基底であるとする. このとき $G = H$ が成り立つ.

係数ブール環上のグレブナ基底は上記の単項式簡約を利用したブッフバーガーアルゴリズムで計算できる.

Algoritm BC
Input: F a finite subset of $\mathbf{B}[\bar{X}]$
Output: F' a set of boolean closed polynomials such that $\langle F\rangle = \langle F'\rangle$
begin
$F' = \emptyset$
while $F \neq \emptyset$ do
select f from F
$F = F \backslash \{f\}$
$F' = F' \cup \{bc(f)\}$
$F = F \cup \{f - bc(f)\}$
end
return F'

Algoritm GB

Input: F a finite subset of $\mathbf{B}[\bar{X}]$
Output: G a Gröbner basis of $\langle F\rangle$ w.r.t $>$
bigin
$G = BC(F)$
while
　　$G' = G$
　　for each pair $\{p,q\}(p,q \in G', p \neq q)$ do
　　　　h = a normal form of $S(p,q)$ modulo G' i.e. $S(p,q) \xrightarrow{*}_G h$
　　　　if $h \neq 0$ then $G = G \cup \{h\}$
$G = G'$ do
end
ブーリアングレブナ基底に関しても今までの定義や定理と同じような議論ができる．またアルゴリズムも非常にシンプルである．

定義 7 ブール多項式環 $\mathbf{B}(\bar{X})$ のイデアル I に対して,I の有限部分集合 G が I のブーリアングレブナ基底であるとは $\langle LM(I)\rangle = \langle LM(G)\rangle$ を満たすことである．

　　Algoritm BGB
Input: F a finite subset of $\mathbf{B}(X_1,\ldots,X_n)$
Output: G a boolean Gröbner basis of $\langle F\rangle$ w.r.t $>$
begin
G =GB$(F \cup \{X_1^2 - X_1,\ldots,X_n^2 - X_n\})(X_1^2 - X_1,\ldots,X_n^2 - X_n \in \mathbf{B}[\bar{X}])$
$G = G\backslash\{X_1^2 - X_1,\ldots,X_n^2 - X_n\}$
end
return G

4　最小多項式

最小多項式を次のように定義する．

定義 8 I をブール多項式環 $\mathbf{B}(\bar{X})$ のイデアルとする．それぞれの変数 X_i に対して、一変数ブール多項式 $f(X_i)$ が $I \cap \mathbf{B}(X_i) = \langle f(X_i)\rangle$ を満たすとき $f(X_i)$ を I に関する X_i の最小多項式と呼ぶ．

$\mathbb{GF}_2$ 上での最小多項式の計算は容易である．

補題 1 $I \subseteq \mathbb{GF}_2(\bar{X})$ をイデアルとし,G を任意の単項式順序での I の簡約ブーリアングレブナ基底とする．I が最小多項式 $f(X_i)$ を含むならば G は $f(X_i)$ を含む．

我々はブーリアングレブナ基底を集合制約問題に応用する過程で、ブーリアングレブナ基底の中から almost solution polynomials を見つけ出すことの重要性を発見した．この almost solution polynomials を使うことで、ブール多項式環上での最小多項式に対して次の定理が得られた．

定理 4 $I \subseteq \mathbf{B}(\bar{X})$ をイデアルとし,G を任意の単項式順序での I の *stratified* ブーリアングレブナ基底とする．$I \cap \mathbf{B}(X_i) = \langle aX_i + b\rangle$ ならば G は $g = cX_i + d_1t_1 + \cdots + d_lt_l + e$ を含む．ただし $LT(g) = X_i$、$c(1 + d_1 \vee \cdots \vee d_l) = a$、$e(1 + d_1 \vee \cdots \vee d_l) = b$ とする．

5 まとめ

本研究によりブール多項式環上での一変数最小多項式は任意の単項式順序でのブーリアングレブナ基底から求めることができることが分かった. 今後は集合の要素数に関する他の条件に対しても、ブーリアングレブナ基底を有効的に活用していきたい.

[1] Inoue, S.(2009). BGSet - a software to compute Boolean Gröbner bases -. http://www.mi.kagu.tus.ac.jp/ inoue/BGSet

[2] Inoue, S.(2009). On the Computation of Comprehensive Boolean Gröbner Bases. Proceedings of the 11th International Workshop on Computer Algebra in Scientific Computing(CASC 2009), LNCS 5743, pp 130-141, Springer-Verlag Berlin Heidelberg.

[3] Sakai, K. and Sato, Y. (1988). Boolean Gröbner bases. ICOT Technical Momorandum 488. http://www.icot.or.jp/ARCHIVE/Museum/TRTM/tm-list-E.html

[4] Sakai, K., Sato, Y. and Menju, S. (1991). Boolean Gröbner bases(revised). ICOT Technical Report 613. http://www.icot.or.jp/ARCHIVE/Museum/TRTM/tr-list-E.html

[5] Sato, Y. et al.(1996). Set Constrains Solvers(Prolog version). http://www.jipdec.jp/icot/ARCHIVE/Museum/FUNDING/funding-95-E.html

[6] Sato, Y.(1998). A new type of canonical Gröbner bases in polynomial rings over Von Neumann regular rings. Proceedings of ISSAC 1998, ACM Press, pp 317-32.

[7] Sato, Y. et al.(1998). Set Constrains Solvers(Klic version). http://www.jipdec.jp/icot/ARCHIVE/Museum/FUNDING/funding-98-E.html

[8] Sato, Y., Nagai, A. and Inoue, I.(2008). On the Computation of Elimination Ideals of Boolean Polynomial Rings, LNAI 5081, pp 338-348, Springer-Verlag Berlin Heidelberg.

[9] Weispfenning, V. (1989). Gröbner bases in polynomial ideals over commutative regular rings. In Davenport Ed., editor, *EUROCAL'87*, pp 336-347. Springer LNCS 378, 1989.